UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,621	04/26/2001	Harald Vater	JEK/YATER	8124

23364 7590 07/19/2004

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	6

DATE MAILED: 07/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/763,621	Applicant(s) VATER ET AL.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. In response to communications filed on 4/26/2001, applicant has pre-amended claims 3, 4, 6, 7, 11, 12, 15, 16, and 18. Pursuant to USC 131, claims 1-18 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: "EXOR" should be replaced with --XOR--, on pages 5-6. Appropriate correction is required.

Claim Objections

3. **Claims 3 and 11** are objected to because of the following informalities: "EXOR" should be replaced with --XOR--. Appropriate correction is required.

Claims 1 and 9 and the intervening claims are objected to because of the following informalities: in claim 1, "the" undisguised operation (h) on the last line should be revised. With respect to claim 9, "the" disguised operation on the third and 4th paragraphs should be corrected. Appropriate correction is required. Applicant is requested to review the claims in correcting similar errors.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. For instance the limitations in the independent claims 1 and 9 refer to a claimed process of manipulating mathematical algorithm without being limited to a practical application. See MPEP § 2106 paragraph IV.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5.1 **Claims 1, 2, 4, 6, 7, 8, and 18** are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 5,153,581 to **Saada et al.**.

5.2 **As per claim 1, Saada et al.** substantially discloses a data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that the operation (h) is disguised before its execution, for example (see column 7, lines 37-60), the disguised operation (h R_1) is executed with disguised input data (x O R_1) , for example (see column 8, lines 26-47 and column 9, lines 49-60), and the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h R_1) with disguised input data (x

O R,) yields output data (y) identical with the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x), for example (see column 8, lines 26-47).

As per claim 2, **Saada et al.** discloses the limitation of a data carrier characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h R_1) and the disguised input data (x O R_1), for example (see column 8, lines 26-47).

As per claim 4, **Saada et al.** discloses the limitation of a data carrier characterized in that the disguised operation (h R_1) is permanently stored in the data carrier in advance, for example (see column 7, lines 37-45).

As per claim 6, **Saada et al.** discloses the limitation of a data carrier characterized in that the disguised operation (h $R_1$is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation, for example (see column 3, lines 30-67).

As per claim 7, **Saada et al.** discloses the limitation of a data carrier characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y), for example (see drawings).

As per claim 8, Saada et al. discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1), for example (see column 8, lines 26-47).

As per claim 18, Saada et al. discloses the limitation of a data carrier characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h), for example (see column 9, lines 49-58 and lines 1-5).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 3, 5, and 9-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,549,075 to **Saada et al.** in view of Bruce **Schneier**, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, Pages 349-353, 366-367.

6.2 **As per claims 3, 9, and 11, claim 9** is similar to claim 1 except for including a XORing operation to the input to yield a new output. However, **Schneier** in an analogous art teaches the technique of XORing some key material of the input and Xoring some other key material with the advantage of low cost and attack prevention, for example (see pages 366-367). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Saada et al.** to provide a technique of XORing the input and output as it is cheap and prevents attack from cryptanalyst as taught by **Schneier**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Schneier** so as to provide a technique with a low cost and at the same time preventing attack from cryptanalysts.

As per claim 10, Saada et al. discloses the limitation of a data carrier characterized in that at least one random number (R_1) enters into the determination of the disguised input data (x O R_1) and at least two random numbers (R_1R_2) enter into the determination of the disguised operations (h R_1R_2), for example (see column 9, lines 47-55).

As per claim 12, Saada et al. discloses the limitation of a data carrier characterized in that the disguised operation (h R_1R_2) is permanently stored in the data carrier in advance, for example (see column 7, lines 37-45).

As per claims 5 and 13, Saada et al. discloses the limitation of a data carrier characterized in that at least two disguised operations (h R_1R_2, h $R_1{\cdot}R_2{\cdot}$) are permanently stored

in the data carrier in advance and one of the stored disguised operations (h R_1R_2, h $R_1{\cdot}R_2{\cdot}$) is selected randomly when a disguised operation is to be executed, for example (see column 2, lines 21-58). **Saada et al.** suggests using random for protection. **Schneier** in an analogous art teaches randomly selecting S-box, which is a mapping of inputs and outputs, for example (see pages 349-353). Therefore claim 13 is rejected on the same rationale as the rejection of claim 9.

As per claim 14, Saada et al. discloses the limitation of a data carrier characterized in that the random numbers (R_1R_2) for determining the first disguised operation (h R_1R_2) are inverse to the random numbers ($R_1{\cdot}R_2{\cdot}$) for determining the second disguised operation (h $R_1{\cdot}R_2{\cdot}$) with respect to the combination used for determining the disguised operations (h R_1R_2, h $R_1{\cdot}R_2{\cdot}$). **Saada et al.** discloses using two random numbers that can be the same or different, for example (see column 9, lines 47-55. It is obvious to one skilled in the art that using inverse random numbers will not depart from the spirit and scope of the invention disclosed by **Saada et al.**.

As per claim 15, Saada et al. discloses the limitation of a data carrier characterized in that the disguised operation (h R_1R_2) is recalculated before its execution and the random numbers (R_1R_2) are redetermined for said calculation, for example (see column 3, lines 30-67).

As per claim 16, Saada et al. discloses the limitation of a data carrier characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y), for example (see drawings).

As per claim 17, Saada et al. discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2), for example (see drawings; see column 9, lines 47-55 and rejection of claim 9).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the a data carrier able to perform operation which is at least a function of a secret key and a random number. US Patent: 5,153,581 Hazard

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Cc

Carl Colin

Patent Examiner
July 9, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100